AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS:

1-19. (canceled)

20. (new) A method for digitally signing a form of a user of a server in an information network comprising both an open and a closed network, the method comprising:

- sending from a user's terminal of the open network a signature request concerning the form to be digitally signed to a closed-network service provider via an open-network service provider, and further to a user's terminal of the closed network,

- accepting said signature request by entering a code at the user's terminal of the closed network,

- transferring said accepted signature request to the open-network service provider via the closed-network service provider, and further to the user's terminal of the open network in order to connect said accepted signature request to said form to be digitally signed, and

- wherein the service provider of the closed network offers verification service to the receiver of the digitally

signed form in order to verify the authenticity of the digitally signed form.

21. (new) The method according to claim 20, wherein the parties associated with the transfer of data are identified by a service provider.

22. (new) The method according to claim 20, wherein the parties associated with the transfer of data are identified by a reliable third party.

23. (new) The method according to claim 20, wherein said code entered at a terminal is a PIN code that can be authenticated by a SIM card.

24. (new) The method according to claim 20, wherein the decryption of data related to said transaction is performed using a service user's terminal.

25. (new) The method according to claim 20, wherein the data related to the acceptance of said transaction are encrypted using a service user's terminal.

26. (new) An arrangement for digitally signing a form of a user of a server in an information network, the arrangement

comprising an open and a closed information network method, the arrangement further comprising:

- means adapted to send from a user's terminal of the open network a signature request concerning the form to be digitally signed to a closed-network service provider via an open-network service provider, and further to a user's terminal of the closed network,

- means for accepting said signature request by entering a code at the user's terminal of the closed network,

- means adapted to transfer said accepted signature request to the open-network service provider via the closed-network service provider, and further to the user's terminal of the open network in order to connect said accepted signature request to said form to be digitally signed, and

- wherein the service provider of the closed network is adapted to offer verification service to the receiver of the digitally signed form in order to verify the authenticity of the digitally signed form.

27. (new) The arrangement according to claim 26, wherein said arrangement further comprises means for identifying and authenticating said code entered at a terminal.

28. (new) The arrangement according to claim 26, wherein said closed network is a mobile telephone network.

29. (new) The arrangement according to claim 20, wherein said open network is the Internet.

30. (new) The arrangement according to claim 20, wherein said terminal of a closed network is a wireless terminal.

31. (new) The arrangement according to claim 30, wherein Said terminal has a SIM card.

32. (new) The arrangement according to claim 31, wherein an encryption key is stored on the SIM card of said terminal.

33. (new) The arrangement according to claim 30, wherein said terminal has a processor for encrypting and decrypting data.